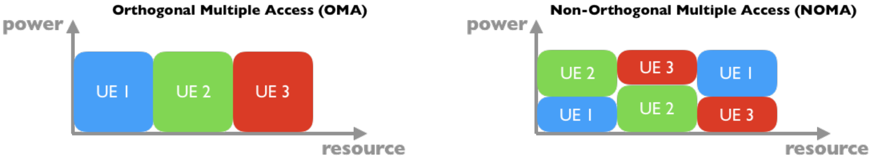
Securing Downlink Non-Orthogonal Multiple Access Systems by Trusted Relays

Ahmed Arafa[1] Wonjae Shin[2,1] Mojtaba Vaezi[3] H. Vincent Poor[1]

[1]Electrical Engineering Department, Princeton University, USA
[2]Department of Electronics Engineering, Pusan National University, South Korea
[3]Electrical and Computer Engineering Department, Villanova University, USA

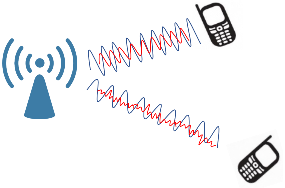
12/10/2018

Non-Orthogonal Multiple Access (NOMA)



- NOMA techniques offer solutions to spectrum scarcity and congestion problems.
- **Key feature:** efficient utilization of available resources serving multiple users *simultaneously* over the same resource: frequency, time, code, or space.
- Vulnerable to eavesdropping (wireless communications inherent openness).
- **How to provide security guarantees with multiple interfering users?**

- Traditionally a higher-layer issue: encryption, key distribution...
- Might be insufficient with the increasing computational powers of adversarial nodes/eavesdroppers.

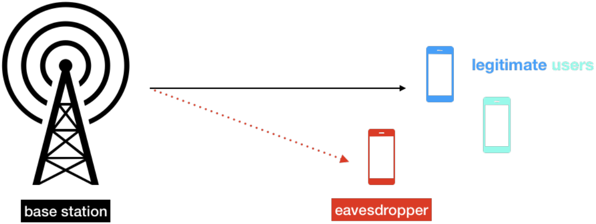


- Physical layer security provides security by exploiting the imperfections in the physical communication channel: noise, fading, interference...
- Joint encoding for security and reliability.

Physical Layer Security for NOMA—Related Works

- SISO secrecy sum rate maximization: [**Zhang** - **Wang** - **Yang** - **Ding** '16].
- Large-scale security for downlink: [**liu** - **Qin** - **Elkashlan** - **Gao** - **Hanzo** '17]; and uplink: [**Gomez** - **Martin-Vega** - **Lopez-Martinez** - **Liu** - **Elkashlan** '17].
- NOMA-assisted multicast-unicast streaming: [**Ding** - **Zhao** - **Peng** - **Poor** '17].
- MIMO secrecy sum rate: [**Tian** - **Zhang** - **Zhao** - **Li** - **Qin** '17].
- One user is untrusted with MISO: [**Li** - **Jiang** - **Zhang** - **Li** - **Qin** '17]; and MIMO: [**Jiang** - **Li** - **Zhang** - **Li** - **Qin** '17].
- Transmit antenna selection: [**Lei** - **Zhang** - **Park** - **Xu** - **Ansari** - **Pan** - **Alomair** - **Alouini** '17].
- Secrecy rate maximization with outage probability constraints: [**He** - **Liu** - **Yang** - **Lau** '17].
- . . .

Typical NOMA Downlink Setting

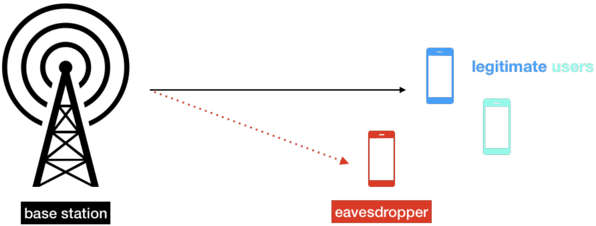


- BS uses superposition coding to send two messages to the legitimate users:

$$x = \sqrt{\alpha P} s_1 + \sqrt{\bar{\alpha} P} s_2$$

- Strong user decodes both messages using successive interference cancellation.
- Weak user decodes its message by treating interference as noise.
- An external eavesdropper wiretaps the communication.

Typical NOMA Downlink Setting

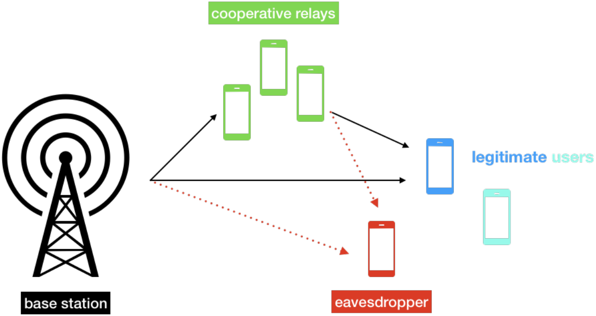


- Secrecy capacities of this multi-receiver wiretap channel [**Ekrem-Ulukus** '11]:

$$r_{s,1} = \left[\log\left(1 + |h_1|^2 \alpha P\right) - \log\left(1 + |h_e|^2 \alpha P\right)\right]^+$$

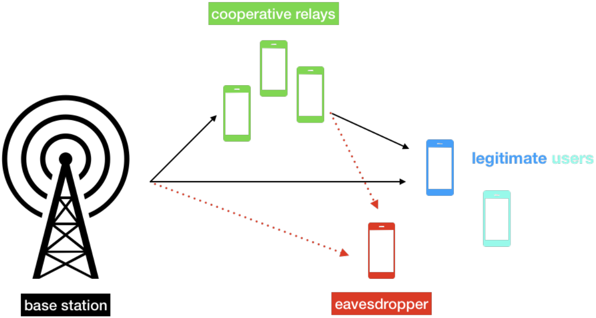
$$r_{s,2} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P}\right)\right]^+$$

This Paper: Employing Trusted Relays to Secure a NOMA Downlink...



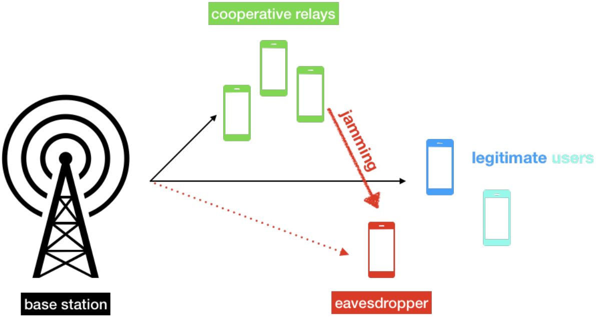
- How can a number of *trusted cooperative* relays enhance the secrecy rate region?

System Model



- Channels are complex-valued, fixed, and known. Noise is $\sim \mathcal{CN}(0, 1)$.
- K relays, half-duplex, trusted, and cooperative.
- Each node is equipped with a single-antenna (SISO).
- BS reduces its power to $\bar{P}$; relays share the remaining $P - \bar{P}$.
- Three relaying schemes:
  cooperative jamming, decode-and-forward and amplify-and-forward.

Relaying Scheme 1: Cooperative Jamming



- Relays transmit a jamming signal $\boldsymbol{J}z$ *simultaneously* with the BS's transmission.
- $z \sim \mathcal{CN}(0,1)$; $\boldsymbol{J} \in \mathbb{C}^K$ is a beamforming vector.
- Jamming signal should not affect the legitimate users:

$$[\boldsymbol{g}_1 \quad \boldsymbol{g}_2]^\dagger \boldsymbol{J}_o \triangleq \boldsymbol{G}^\dagger \boldsymbol{J}_o = [0 \quad 0]$$

Relaying Scheme 1: Cooperative Jamming—Achievable Secrecy Rates

- Without relays (direct transmission):

$$r_{s,1} = \left[\log\left(1 + |h_1|^2 \alpha P\right) - \log\left(1 + |h_e|^2 \alpha P\right)\right]^+$$

$$r_{s,2} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P}\right)\right]^+$$

Relaying Scheme 1: Cooperative Jamming—Achievable Secrecy Rates

- With cooperative jamming:

$$r_{s,1}^{J} = \left[\log\left(1+|h_1|^2\alpha\bar{P}\right) - \log\left(1+\frac{|h_e|^2\alpha\bar{P}}{1+|\boldsymbol{g}_e{}^{\dagger}\boldsymbol{J}_o|^2}\right)\right]^{+}$$

$$r_{s,2}^{J} = \left[\log\left(1+\frac{|h_2|^2\bar{\alpha}\bar{P}}{1+|h_2|^2\alpha\bar{P}}\right) - \log\left(1+\frac{|h_e|^2\bar{\alpha}\bar{P}}{1+|h_e|^2\alpha\bar{P}+|\boldsymbol{g}_e{}^{\dagger}\boldsymbol{J}_o|^2}\right)\right]^{+}$$

- Best beamforming vector:

$$\begin{aligned}
\max_{\boldsymbol{J}_o} \quad & \left|\boldsymbol{g}_e^{\dagger}\boldsymbol{J}_o\right|^2 \\
\text{s.t.} \quad & \boldsymbol{G}^{\dagger}\boldsymbol{J}_o = [0 \quad 0] \\
& \boldsymbol{J}_o^{\dagger}\boldsymbol{J}_o = P - \bar{P}
\end{aligned}$$

- Unique solution:

$$\boxed{\hat{\boldsymbol{J}}_o = \frac{\mathcal{P}^{\perp}(\boldsymbol{G})\,\boldsymbol{g}_e}{\left\|\mathcal{P}^{\perp}(\boldsymbol{G})\,\boldsymbol{g}_e\right\|}\sqrt{P-\bar{P}}}$$

- $\mathcal{P}^{\perp}(\cdot)$ is a projection matrix:

$$\mathcal{P}^{\perp}(\boldsymbol{G}) \triangleq \boldsymbol{I}_K - \boldsymbol{G}\left(\boldsymbol{G}^{\dagger}\boldsymbol{G}\right)^{-1}\boldsymbol{G}^{\dagger}$$

Relaying Scheme 1: Cooperative Jamming—Achievable Secrecy Rates

- With cooperative jamming:

$$r^J_{s,1} = \left[\log\left(1 + |h_1|^2 \alpha \bar{P}\right) - \log\left(1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + |\boldsymbol{g}_e{}^\dagger \boldsymbol{J}_o|^2}\right)\right]^+$$

$$r^J_{s,2} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P} + |\boldsymbol{g}_e{}^\dagger \boldsymbol{J}_o|^2}\right)\right]^+$$

  - Best beamforming vector:

$$\max_{\boldsymbol{J}_o} \quad \left|\boldsymbol{g}_e^\dagger \boldsymbol{J}_o\right|^2$$
$$\text{s.t.} \quad \boldsymbol{G}^\dagger \boldsymbol{J}_o = [0 \quad 0]$$
$$\boldsymbol{J}_o^\dagger \boldsymbol{J}_o = P - \bar{P}$$

- Unique solution:

$$\boxed{\hat{\boldsymbol{J}}_o = \frac{\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e}{\left\|\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e\right\|}\sqrt{P - \bar{P}}}$$

- $\mathcal{P}^\perp(\cdot)$ is a projection matrix:

$$\mathcal{P}^\perp(\boldsymbol{G}) \triangleq \boldsymbol{I}_K - \boldsymbol{G}\left(\boldsymbol{G}^\dagger \boldsymbol{G}\right)^{-1} \boldsymbol{G}^\dagger$$

- With cooperative jamming:

$$r_{s,1}^{J} = \left[\log\left(1 + |h_1|^2 \alpha \bar{P}\right) - \log\left(1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + |\boldsymbol{g}_e{}^{\dagger} \boldsymbol{J}_o|^2}\right)\right]^+$$

$$r_{s,2}^{J} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P} + |\boldsymbol{g}_e{}^{\dagger} \boldsymbol{J}_o|^2}\right)\right]^+$$

- Best beamforming vector:

$$\max_{\boldsymbol{J}_o} \quad \left|\boldsymbol{g}_e^{\dagger} \boldsymbol{J}_o\right|^2$$
$$\text{s.t.} \quad \boldsymbol{G}^{\dagger} \boldsymbol{J}_o = [0 \quad 0]$$
$$\boldsymbol{J}_o^{\dagger} \boldsymbol{J}_o = P - \bar{P}$$

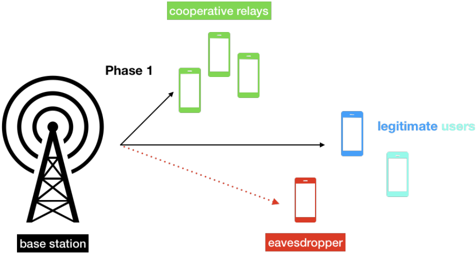
- Unique solution:

$$\boxed{\hat{\boldsymbol{J}}_o = \frac{\mathcal{P}^{\perp}(\boldsymbol{G})\, \boldsymbol{g}_e}{\|\mathcal{P}^{\perp}(\boldsymbol{G})\, \boldsymbol{g}_e\|} \sqrt{P - \bar{P}}}$$

- $\mathcal{P}^{\perp}(\cdot)$ is a projection matrix:

$$\mathcal{P}^{\perp}(\boldsymbol{G}) \triangleq \boldsymbol{I}_K - \boldsymbol{G}\left(\boldsymbol{G}^{\dagger} \boldsymbol{G}\right)^{-1} \boldsymbol{G}^{\dagger}$$

Relaying Scheme 2: Decode-and-Forward



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.
- In what order should the kth relay decode? *Depends on operating point...*
  - (1): strong user's message first:

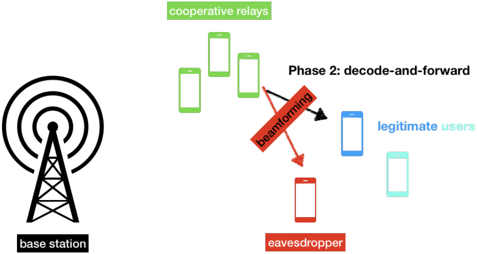
    $$R_{k,1}^{(1)} = \log\left(1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}}\right)$$

    $$R_{k,2}^{(1)} = \log\left(1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}\right)$$
  - (2): weak user's message first:

    $$R_{k,1}^{(2)} = \log\left(1 + |h_{r,k}|^2 \alpha \bar{P}\right)$$

    $$R_{k,2}^{(2)} = \log\left(1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}}\right)$$

Relaying Scheme 2: Decode-and-Forward



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.
- In what order should the kth relay decode? *Depends on operating point...*
  - (1): strong user's message first:

$$R_{k,1}^{(1)} = \log\left(1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}}\right)$$

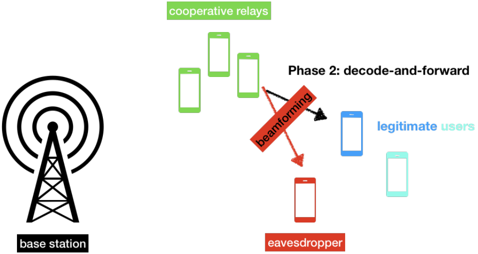
$$R_{k,2}^{(1)} = \log\left(1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}\right)$$

  - (2): weak user's message first:

$$R_{k,1}^{(2)} = \log\left(1 + |h_{r,k}|^2 \alpha \bar{P}\right)$$

$$R_{k,2}^{(2)} = \log\left(1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}}\right)$$

Relaying Scheme 2: Decode-and-Forward



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.
- In what order should the kth relay decode? *Depends on operating point...*
  - (1): strong user's message first:

    $$R_{k,1}^{(1)} = \log\left(1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}}\right)$$

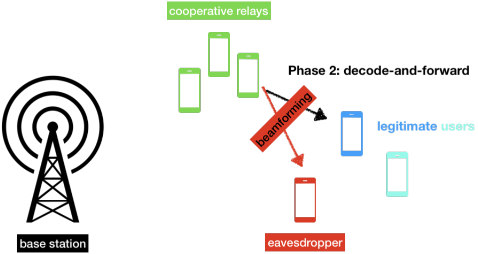
    $$R_{k,2}^{(1)} = \log\left(1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}\right)$$

  - (2): weak user's message first:

    $$R_{k,1}^{(2)} = \log\left(1 + |h_{r,k}|^2 \alpha \bar{P}\right)$$

    $$R_{k,2}^{(2)} = \log\left(1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}}\right)$$

Relaying Scheme 2: Decode-and-Forward



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.

- In what order should the kth relay decode? *Depends on operating point...*

  - (1): strong user's message first:

$$R_{k,1}^{(1)} = \log\left(1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}}\right)$$

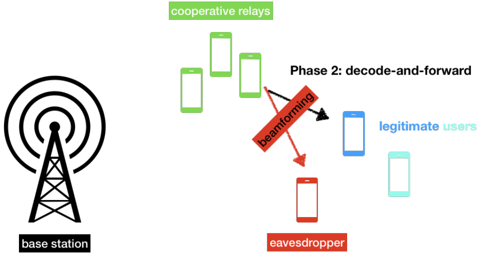
$$R_{k,2}^{(1)} = \log\left(1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}\right)$$

  - (2): weak user's message first:

$$R_{k,1}^{(2)} = \log\left(1 + |h_{r,k}|^2 \alpha \bar{P}\right)$$

$$R_{k,2}^{(2)} = \log\left(1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}}\right)$$

Relaying Scheme 2: Decode-and-Forward



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.
- In what order should the kth relay decode? *Depends on operating point...*
  - (1): strong user's message first:

$$R_{k,1}^{(1)} = \log\left(1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}}\right)$$

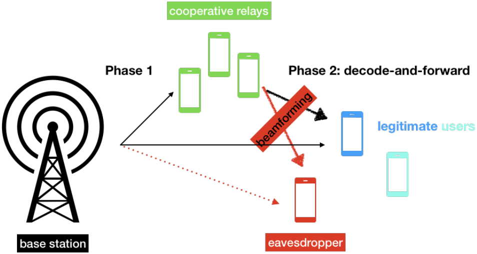
$$R_{k,2}^{(1)} = \log\left(1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}\right)$$

  - (2): weak user's message first:

$$R_{k,1}^{(2)} = \log\left(1 + |h_{r,k}|^2 \alpha \bar{P}\right)$$

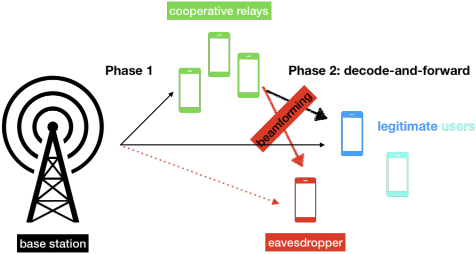
$$R_{k,2}^{(2)} = \log\left(1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}}\right)$$

Relaying Scheme 2: Decode-and-Forward



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.
- Eavesdropper overhears communication in both phases.
- Eliminate eavesdropping benefit in **Phase 2:**

$$\boldsymbol{g}_e{}^\dagger \boldsymbol{d}_o = 0$$



- Communication occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $\boldsymbol{d} \in \mathbb{C}^K$.
- Eavesdropper overhears communication in both phases.
- Eliminate eavesdropping benefit in **Phase 2:**

$$\boldsymbol{g}_e{}^{\dagger}\boldsymbol{d}_o = 0$$

Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

- Without relays (direct transmission):

$$r_{s,1} = \left[\log\left(1 + |h_1|^2 \alpha P\right) - \log\left(1 + |h_e|^2 \alpha P\right)\right]^+$$

$$r_{s,2} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P}\right)\right]^+$$

Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

- With decode-and-forward:

$$r_{s,1}^{DF} = \frac{1}{2}\left[r_1^{DF} - \log\left(1 + |h_e|^2 \alpha \bar{P}\right)\right]^+$$

$$r_{s,2}^{DF} = \frac{1}{2}\left[r_2^{DF} - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P}}\right)\right]^+$$

where

$$r_1^{DF} = \min\left\{\log\left(1 + |h_1|^2 \alpha \bar{P}\right) + \log\left(1 + \left|\boldsymbol{g}_1{}^\dagger \boldsymbol{d}_o\right|^2 \alpha\left(P - \bar{P}\right)\right), \min_{1 \le k \le K} R_{k,1}^{(i)}\right\}$$

$$r_2^{DF} = \min\left\{\log\left(1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}}\right) + \log\left(1 + \frac{\left|\boldsymbol{g}_2{}^\dagger \boldsymbol{d}_o\right|^2 \bar{\alpha}\left(P - \bar{P}\right)}{1 + \left|\boldsymbol{g}_2{}^\dagger \boldsymbol{d}_o\right|^2 \alpha\left(P - \bar{P}\right)}\right), \min_{1 \le k \le K} R_{k,2}^{(i)}\right\}$$

- Secrecy rates depend on decoding order (i), $i = 1, 2$, at the relays.
- Extra $\frac{1}{2}$ terms are due to sending same information over two phases.

Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

- With decode-and-forward:

$$r_{s,1}^{DF} = \frac{1}{2}\left[r_1^{DF} - \log\left(1 + |h_e|^2 \alpha \bar{P}\right)\right]^+$$

$$r_{s,2}^{DF} = \frac{1}{2}\left[r_2^{DF} - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P}}\right)\right]^+$$

where

$$r_1^{DF} = \min\left\{\log\left(1 + |h_1|^2 \alpha \bar{P}\right) + \log\left(1 + \left|\boldsymbol{g}_1{}^{\dagger} \boldsymbol{d}_o\right|^2 \alpha\left(P - \bar{P}\right)\right), \min_{1 \le k \le K} R_{k,1}^{(i)}\right\}$$

$$r_2^{DF} = \min\left\{\log\left(1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}}\right) + \log\left(1 + \frac{\left|\boldsymbol{g}_2{}^{\dagger} \boldsymbol{d}_o\right|^2 \bar{\alpha}\left(P - \bar{P}\right)}{1 + \left|\boldsymbol{g}_2{}^{\dagger} \boldsymbol{d}_o\right|^2 \alpha\left(P - \bar{P}\right)}\right), \min_{1 \le k \le K} R_{k,2}^{(i)}\right\}$$

- Fix $0 \le \beta \le 1$.
- Proposed beamforming vector:

$$\begin{aligned} \max_{\boldsymbol{d}_o} \quad & \beta\left|\boldsymbol{g}_1^{\dagger} \boldsymbol{d}_o\right|^2 + (1 - \beta)\left|\boldsymbol{g}_2^{\dagger} \boldsymbol{d}_o\right|^2 \\ \text{s.t.} \quad & \boldsymbol{g}_e^{\dagger} \boldsymbol{d}_o = 0 \\ & \boldsymbol{d}_o^{\dagger} \boldsymbol{d}_o = 1 \end{aligned}$$

- Unique solution:

$$\boxed{\hat{\boldsymbol{d}}_o = \frac{\mathcal{P}^{\perp}(\boldsymbol{g}_e)\,\hat{\mathbf{u}}_d}{\|\mathcal{P}^{\perp}(\boldsymbol{g}_e)\,\hat{\mathbf{u}}_d\|}}$$

- $\hat{\mathbf{u}}_d$: leading eigenvector of

$$\mathcal{P}^{\perp}(\boldsymbol{g}_e)\left(\beta \boldsymbol{g}_1 \boldsymbol{g}_1^{\dagger} + (1 - \beta)\boldsymbol{g}_2 \boldsymbol{g}_2^{\dagger}\right)\mathcal{P}^{\perp}(\boldsymbol{g}_e)$$

Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

- With decode-and-forward:

$$
\begin{aligned}
r_{s,1}^{DF} &= \frac{1}{2}\left[r_1^{DF} - \log\left(1 + |h_e|^2 \alpha \bar{P}\right)\right]^+ \\
r_{s,2}^{DF} &= \frac{1}{2}\left[r_2^{DF} - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P}}\right)\right]^+
\end{aligned}
$$

where

$$
r_1^{DF} = \min\left\{\log\left(1 + |h_1|^2 \alpha \bar{P}\right) + \log\left(1 + \left|\boldsymbol{g}_1{}^\dagger \boldsymbol{d}_o\right|^2 \alpha\left(P - \bar{P}\right)\right), \min_{1 \le k \le K} R_{k,1}^{(i)}\right\}
$$

$$
r_2^{DF} = \min\left\{\log\left(1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}}\right) + \log\left(1 + \frac{\left|\boldsymbol{g}_2{}^\dagger \boldsymbol{d}_o\right|^2 \bar{\alpha}\left(P - \bar{P}\right)}{1 + \left|\boldsymbol{g}_2{}^\dagger \boldsymbol{d}_o\right|^2 \alpha\left(P - \bar{P}\right)}\right), \min_{1 \le k \le K} R_{k,2}^{(i)}\right\}
$$

- Fix $0 \le \beta \le 1$.
- Proposed beamforming vector:

$$
\begin{aligned}
\max_{\boldsymbol{d}_o} \quad & \beta\left|\boldsymbol{g}_1^\dagger \boldsymbol{d}_o\right|^2 + (1-\beta)\left|\boldsymbol{g}_2^\dagger \boldsymbol{d}_o\right|^2 \\
\text{s.t.} \quad & \boldsymbol{g}_e^\dagger \boldsymbol{d}_o = 0 \\
& \boldsymbol{d}_o^\dagger \boldsymbol{d}_o = 1
\end{aligned}
$$

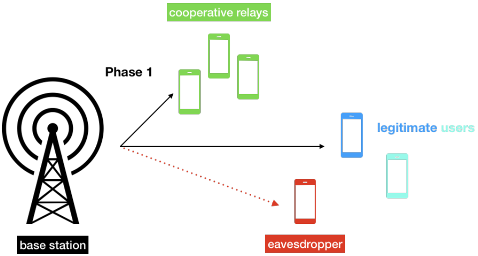
- Unique solution:

$$
\boxed{\hat{\boldsymbol{d}}_o = \frac{\mathcal{P}^\perp(\boldsymbol{g}_e)\,\hat{\boldsymbol{u}}_d}{\|\mathcal{P}^\perp(\boldsymbol{g}_e)\,\hat{\boldsymbol{u}}_d\|}}
$$

- $\hat{\boldsymbol{u}}_d$: leading eigenvector of

$$
\mathcal{P}^\perp(\boldsymbol{g}_e)\left(\beta \boldsymbol{g}_1 \boldsymbol{g}_1^\dagger + (1-\beta)\boldsymbol{g}_2 \boldsymbol{g}_2^\dagger\right)\mathcal{P}^\perp(\boldsymbol{g}_e)
$$

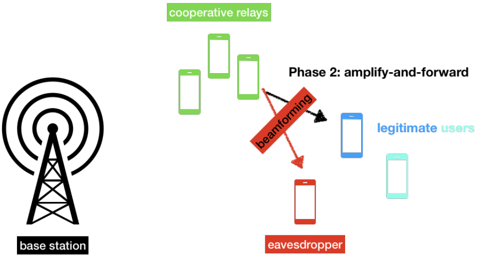
Relaying Scheme 3: Amplify-and-Forward



- Communication also occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays multiply their received signal $\boldsymbol{y}_r$ by a beamforming vector $\boldsymbol{a} \in \mathbb{C}^K$ and forward to users.
- Eavesdropper overhears communication in both phases.
- Eliminate eavesdropping benefit in **Phase** 2:

$$\boldsymbol{g}_e^{\dagger} \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o = 0$$

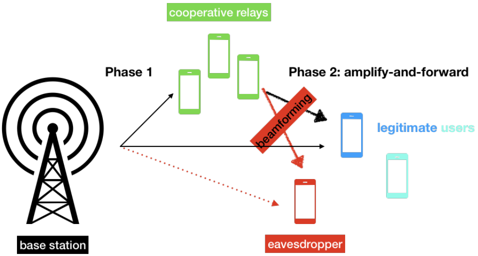
Relaying Scheme 3: Amplify-and-Forward



- Communication also occurs over two phases:
  - **Phase 1:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2:** Relays multiply their received signal $\boldsymbol{y}_r$ by a beamforming vector $\boldsymbol{a} \in \mathbb{C}^K$ and forward to users.
- Eavesdropper overhears communication in both phases.
- Eliminate eavesdropping benefit in **Phase** 2:

$$\boldsymbol{g}_e{}^{\dagger} \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o = 0$$

Relaying Scheme 3: Amplify-and-Forward



- Communication also occurs over two phases:
  - **Phase** 1**:** BS broadcasts the messages to both relays and legitimate users.
  - **Phase** 2**:** Relays multiply their received signal $\boldsymbol{y}_r$ by a beamforming vector $\boldsymbol{a} \in \mathbb{C}^K$ and forward to users.
- Eavesdropper overhears communication in both phases.
- Eliminate eavesdropping benefit in **Phase** 2:

$$\boldsymbol{g}_e{}^{\dagger} \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o = 0$$

- Without relays (direct transmission):

$$r_{s,1} = \left[\log\left(1 + |h_1|^2 \alpha P\right) - \log\left(1 + |h_e|^2 \alpha P\right)\right]^+$$

$$r_{s,2} = \left[\log\left(1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P}\right) - \log\left(1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P}\right)\right]^+$$

Relaying Scheme 3: Amplify-and-Forward—Achievable Secrecy Rates

- With amplify-and-forward:

$$r_{s,1}^{AF} = \frac{1}{2}\left[\log\left(1 + |h_1|^2\alpha\bar{P} + \frac{\boldsymbol{a}_o^\dagger \boldsymbol{G}_{1,r}\boldsymbol{a}_o}{1+\boldsymbol{a}_o^\dagger \boldsymbol{G}_1 \boldsymbol{a}_o}\alpha\bar{P}\right) - \log\left(1+|h_e|^2\alpha\bar{P}\right)\right]^+$$

$$r_{s,2}^{AF} = \frac{1}{2}\left[\log\left(1 + \frac{|h_2|^2\bar{\alpha}\bar{P}}{1+|h_2|^2\alpha\bar{P}} + \frac{\boldsymbol{a}_o^\dagger \boldsymbol{G}_{2,r}\boldsymbol{a}_o\bar{\alpha}\bar{P}}{1+\boldsymbol{a}_o^\dagger \boldsymbol{G}_2 \boldsymbol{a}_o + \boldsymbol{a}_o^\dagger \boldsymbol{G}_{2,r}\boldsymbol{a}_o\alpha\bar{P}}\right) - \log\left(1+\frac{|h_e|^2(1-\alpha)\bar{P}}{1+|h_e|^2\alpha\bar{P}}\right)\right]^+$$

where

$$\boldsymbol{G}_{j,r} \triangleq \mathtt{diag}\left(\boldsymbol{h}_r{}^*\right)\boldsymbol{g}_j\boldsymbol{g}_j^\dagger \mathtt{diag}\left(\boldsymbol{h}_r\right), \quad j = 1,2$$

$$\boldsymbol{G}_j \triangleq \mathtt{diag}\left(\boldsymbol{g}_j^*\right)\mathtt{diag}\left(\boldsymbol{g}_j\right), \quad j = 1,2$$

- Extra $\frac{1}{2}$ terms are due to sending same information over two phases.

Relaying Scheme 3: Amplify-and-Forward—Achievable Secrecy Rates

- Best beamforming vector for jth user:

$$\boldsymbol{a}_o^{(j)} = \sqrt{\frac{P-\bar{P}}{\boldsymbol{u}_a^{(j)T}\boldsymbol{F}\boldsymbol{A}\boldsymbol{F}\boldsymbol{u}_a^{(j)}}}\boldsymbol{F}\boldsymbol{u}_a^{(j)}$$

where

$$\boldsymbol{F} \triangleq \mathcal{P}^{\perp}(\mathtt{diag}\left(\boldsymbol{h}_r\right)\boldsymbol{g}_e)$$
$$\boldsymbol{A} \triangleq \left(\mathtt{diag}\left(\boldsymbol{h}_r^*\right)\mathtt{diag}\left(\boldsymbol{h}_r\right)\bar{P} + \boldsymbol{I}_K\right)$$

- $\boldsymbol{u}_a^{(1)}$: leading *generalized* eigenvector of

$$\left(\boldsymbol{F}\boldsymbol{G}_{1,r}\boldsymbol{F}\ ,\ \boldsymbol{F}\left(\frac{1}{P-\bar{P}}\boldsymbol{A}+\boldsymbol{G}_1\right)\boldsymbol{F}\right)$$

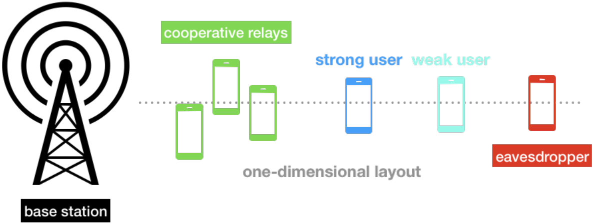
- $\boldsymbol{u}_a^{(2)}$: leading *generalized* eigenvector of

$$\left(\boldsymbol{F}\boldsymbol{G}_{2,r}\boldsymbol{F}\ ,\ \boldsymbol{F}\left(\frac{1}{P-\bar{P}}\boldsymbol{A}+\boldsymbol{G}_2+\boldsymbol{G}_{2,r}\alpha\bar{P}\right)\boldsymbol{F}\right)$$

- Fix $0 \le \beta \le 1$. Proposed beamforming vector:

$$\boxed{\hat{\boldsymbol{a}}_o = \beta\boldsymbol{a}_o^{(1)} + (1-\beta)\boldsymbol{a}_o^{(2)}}$$

Numerical Results—Setup

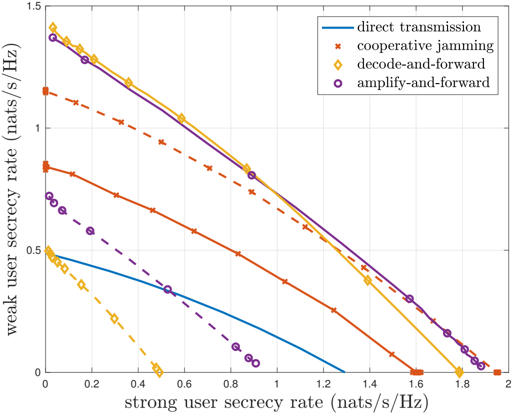


- Characterize the boundary of the secrecy rate region ($n \in \{J, DF, AF\}$):

$$\max_{\alpha, \bar{P}} \quad \mu r_{s,1}^n + (1-\mu) r_{s,2}^n$$
$$\text{s.t.} \quad 0 \le \bar{P} \le P, \quad 0 \le \alpha \le 1$$

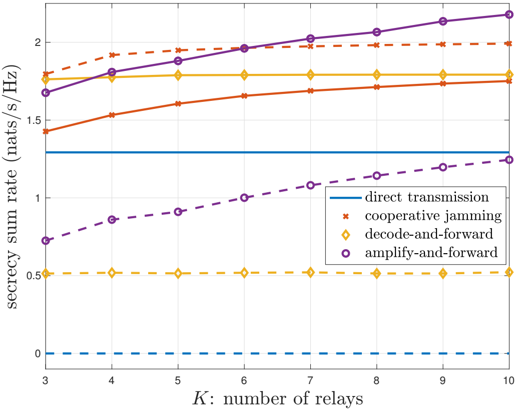
- $K = 5$ relays.
- Pick $\beta = \mu$ for decode-and-forward and amplify-and-forward beamforming vectors.
- Channel gain between two nodes: $h = \sqrt{1/l^\gamma} e^{j\theta}$
  - l: distance between the two nodes.
  - γ: path loss exponent.
  - θ: uniform random variable on $[0, 2\pi]$.

Numerical Results—Secrecy Rate Regions



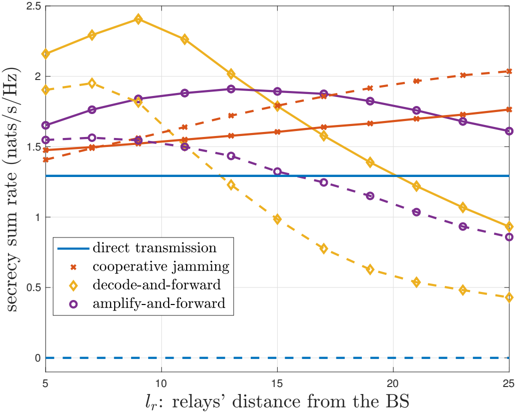
- Dashed lines are when eavesdropper is in between BS and legitimate users; solid lines are when it is beyond them.

Numerical Results—Number of Relays



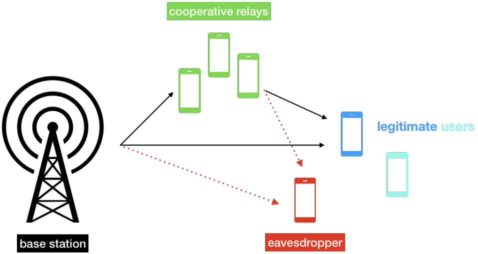
- Dashed lines are when eavesdropper is in between BS and legitimate users; solid lines are when it is beyond them.

Numerical Results—Relays' Location



- Dashed lines are when eavesdropper is in between BS and legitimate users; solid lines are when it is beyond them.

Conclusions



- Considered the relaying benefits on physical layer security of a two-user SISO downlink NOMA with an external eavesdropper.
- **Take-away message:** best relaying scheme depends on relative locations.
- Eextensions:
  - Full-duplex relays.
  - Eavesdropper's channel is unknown.
  - MIMO scenarios.
  - Untrusted relays (presented at **Asilomar '18**).
  - ...